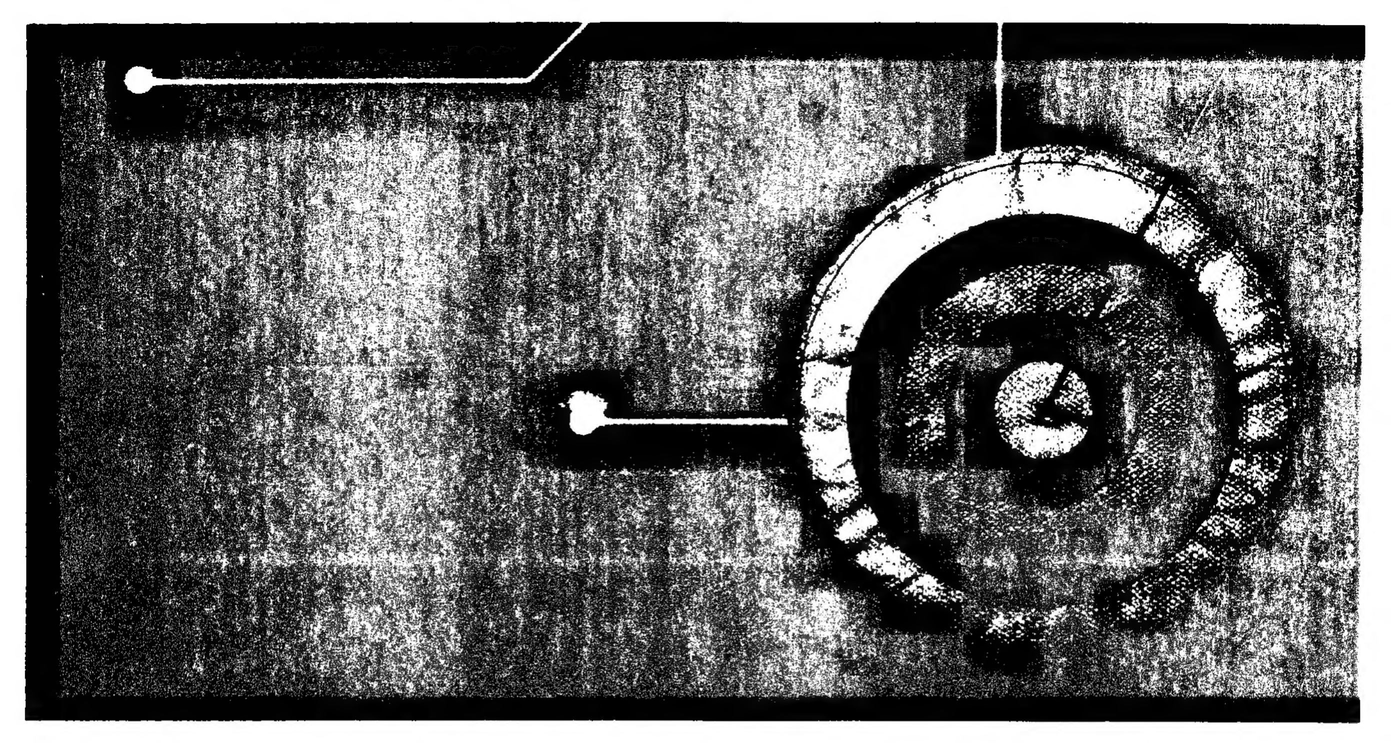


Grundlagen zu Softwareschwächen

Zielscheibe Vulnerability

Beim »Time to Live on the Network«-Experiment wurden ungepatchte Standardsysteme mit dem Internet verbunden und ihre Aktivitäten überwacht. Schon nach wenigen Minuten war das erste System über Software-Schwächen vollständig kompromittiert. Was verbirgt sich hinter diesen Vulnerabities und Exploits, und wie lässt sich diese reale Bedrohung pragmatisch und organisatorisch eindämmen?

Sicherheitslücken sind grundverschieden, haben aber eines gemeinsam: Sie machen ein einzelnes System oder gar ein ganzes Unternehmen anfällig für Angriffe. Die häufigste Ursache der Schwachstellen sind Programmierfehler in verschiedenen Softwareprodukten und Anwendungen. Sicherheitsexperten und Hersteller identifizieren und veröffentlichen jede Woche durchschnittlich 40 solcher Fehler in verschiedenen Produkten – von Betriebssystemen bis hin zu Datenbanken und Anwendungen und sogar Netzwerk-Devices. Typische Beispiele für solche Bugs sind »Buffer-Overflows« in Computerprogrammen. Sie bewirken, dass Teile des Speichers wahllos überschrieben werden. Vergleichen lässt sich diese Aktion mit dem Ausfüllen eines Formulars, in dem für jeden Buchstaben des Namens einer Person ein Feld vorgesehen ist: Wenn nicht genügend Felder vorhanden sind, entsteht das Äquivalent eines Buffer-Overflows bei Computerprogrammen. Ein Buffer-Overflow kann das betroffene Programm zum Absturz bringen oder einem Angreifer sogar die Möglichkeit geben, beliebigen Code auszuführen und auf diese Weise das System zu übernehmen. Aber genauso führen falsch konfigurierte Systeme und Fehlverhalten der Anwender zu Schwächen, die die Gegenseite ausnutzt, Schadencode einzuschleusen.

Jeder neuen Sicherheitslücke wird bei der Bekanntgabe eine eindeutige »Common Vulnerabilities and Exposures«-Nummer (CVE) zugewiesen, damit sie während ihres gesamten Lebenszyklus' präzise kenntlich gemacht ist und man auf sie verweisen kann. Je nach Schweregrad eröffnet eine Sicherheitslücke den Angreifern Wege, ein anfälliges System zum Absturz zu bringen, Zugriff auf vertrauliche Daten zu erlangen oder die Kontrolle über das System zu übernehmen.

Exploits und Angriffe

Exploits sind speziell entwickelte, bösartige Programme, die diese Sicherheitslücken und die darunter leidenden Systeme direkt attackieren. Angreifer wollen mit dem Code ein bestimmtes System ins Visier nehmen und unter ihre Kontrolle bringen. Meist in einer konkreten Absicht, etwa, um vertrauliche Informationen zu

stehlen oder sich finanzielle Vorteile zu verschaffen. Die Saboteure tauschen ihre Exploits aus oder machen sie bekannt, andere greifen sie als Bausteine für eigene Würmer und automatische Angriffe auf. Solche bösartigen Programme können sich dann replizieren und in Netzwerken zirkulieren, um ungepatchte Systeme zu finden. Auf den Wurm Morris aus dem Jahr 1988, einen der ersten automatisierten Angriffe dieser Art, folgten in jüngerer Zeit Slammer, Blaster, Sasser und zahlreiche weitere Würmer, überzeugende Belege dieser Praxis. Abhängig von der spezifischen Nutzlast, die ein Wurm trägt, können sich die Opfer manchmal von dem Angriff erholen. In den meisten Fällen aber müssen die kompromittierten Systeme komplett neu aufgebaut werden, um ihre Systemsicherheit zu gewährleisten.

Ein entscheidender Faktor für die Wirksamkeit eines Exploits ist Zeit – die Geschwindigkeit, in der ein Exploit-Code für eine bestimmte Sicherheitslücke geschrieben und freigesetzt wurde. Die jüngsten automatischen Angriffe ließen die »Time-to-Exploit« von Monaten auf Tage schrumpfen und erfolgten damit schneller als jede menschenmögliche Reaktion. Durch die rasche Entwicklung von Exploits entstehen in Unternehmen lange Anfälligkeitszeiträume bis zur Sicherung der kritischen Systeme. SQL-Slammer trat sechs Monate nach der Entdeckung eines Software-Fehlers auf, Nimda vier Monate, Slapper sechs Wochen danach; Blaster erschien nur drei Wochen, nachdem ein Sicherheitsleck bekannt geworden war, und der Wurm Witty schlug bereits am Tag nach der Bekanntmachung der entsprechenden Schwachstelle zu.

Die in dieser Hinsicht eindrucksvollste Szenerie bot bislang der Wurm Witty, der am 19. März 2004 rund 12000 Rechner befiel, auf denen Firewalls der Firma Internet-Security-Systems liefen. Witty erreichte seinen Gipfelpunkt nach rund 45 Minuten: Zu diesem Zeitpunkt hatte er bereits die meisten anfälligen Hosts infiziert. Laut einer Analyse der CAIDA und der UCSD war Witty gleich in mehrerer Hinsicht ein Novum: Er war der erste weit verbreitete Internet-Wurm, der eine zerstörerische Nutzlast trug; er verbreitete sich auf organisierte Weise mit mehr »Ground-Zero-Hosts« als je zuvor; er steht für das bislang kürzeste Intervall zwischen der Bekanntgabe einer Sicherheitslücke und der Freisetzung eines Wurms (einen Tag); er griff nur Hosts an, auf denen eine Sicherheits-Software lief; und er bewies, dass Anwendungen auf einem Nischenmarkt genau so verletzlich sind wie die Produkte eines Software-Monopolisten.

Pragmatische Gegenmaßnahmen

Sicherheitsattacken auf Netzwerke und Daten werden immer zahlreicher und immer raffinierter. Eine neue Generation automatischer Sicherheitsbedrohungen nützt Lücken schneller aus, als jede menschlichenmögliche Reaktion erfolgen kann. Die rechtzeitige und umfassende Identifizierung von Sicherheitslücken und die schnelle Durchführung von Abhilfemaßnahmen sind das wirksamste vorbeugende Mittel, das Netzwerkmanager ergreifen können, um automatisierte Angriffe abzuwehren und die Datensicherheit zu gewährleisten.

Best-Practices können beim Management und dem Schließen von Sicherheitslücke als Richtschnur dienen und CIOs, Chief-Security-Officers, Netzwerk- und IT-Managern und Sicherheitsspezialisten helfen, den Schutz interner und externer Netze zu verstärken und zu priorisieren. Folgende Sicherheitsstrategien sollten angewandt werden.

Ein kritischer Erfolgsfaktor besteht darin, die Anwender mit praktischen Informationen über Bedrohungen und Abhilfemaßnahmen zu versorgen. Dies geschieht über Schulungen, die die Wachsamkeit der Mitarbeiter wecken. Auch neue, automatische Audit-Lösungen finden alle Anfälligkeiten, identifizieren und priorisieren Sicherheitslücken und bieten geeignete Abhilfemaßnahmen. Deswegen sollte ein Unternehmen regelmäßige Audits der Sicherheitssysteme durchführen.

Bei dem wichtigen Patch-Prozess, den ein Unternehmen unbedingt aufsetzen sollte, müssen die automatischen Lösungen oft manuell unterstützt werden. Nur dann kann der Administrator Systeme reparieren, die er dringend sichern muss. Auch Firewalls und Einbruchsschutzsysteme können dazu beitragen, Angriffe abzuwehren, bevor Eindringlinge ins Netzwerk gelangen. Trendanalysen liefern Daten, um Policies durchzusetzen, und gewährleisten, dass die Sicherheitssysteme den sich ständig wandelnden Angriffsformen gerecht werden.

Schutz vor Exploits

Die rechtzeitige Installation von Security-Patches oder sonstigen Workarounds auf jedem anfälligen System ist ein funktionierender und notwendiger Verteidigungsmechanismus. Er verhindert, dass Exploits ein System angreifen und kompromittieren. Idealerweise liefert der Hersteller den fehlenden Security-Patch, sobald er oder ein anderer eine Sicherheitslücke bekannt macht. Leider ist dies nicht immer so, und eine Schwachstelle wird bekannt, bevor Abhilfemaßnahmen verfügbar sind. In einigen Fällen waren sogar schon Exploits im Umlauf, bevor Patches erhältlich waren. Diese so genannten Zero-Day-Exploits bedeuten ein erhebliches Risiko.

Zum Glück ist das Aufspielen von Security-Patches nicht die einzige Abwehrprozedur. Es gibt Workarounds, die Risiken mindern und die Ausnützung von Sicherheitslecks unterbinden. Einbruchsschutz-Technologien und andere Filtermechanismen tragen dazu bei, Angriffe zu verhindern, ohne dass unverzüglich Patches installiert werden müssen.

Eines der wichtigsten Anliegen eines jeden Unternehmens muss es sein, das richtige Timing zu finden, um anfällige Systeme zu patchen. Manchmal verursacht Patchen Betriebsstörungen und macht Still-

standszeiten notwendig. Auf der anderen Seite erfordern lauernde Exploits dringend Handeln. In den vergangenen beiden Jahren haben sich die Patch-Strategien der Unternehmen erheblich verbessert, und die Firmen entwickeln Metriken, um zu messen, wie ernst und kritisch Sicherheitslücken sind, und so die Dringlichkeit von Abhilfemaßnahmen zu bestimmen. Auch die Tatsache, dass einige Hersteller inzwischen in regelmäßigen Abständen Patches veröffentlichen, trägt dazu bei, das »Patch-des-Tages«-Syndrom aus der Welt zu schaffen, mit dem früher viele Firmen zu kämpfen hatten.

Funktionierendes Schwachstellenmanagement

Um Sicherheitslücken in Netzwerken erfolgreich bekämpfen zu können, muss man ganz genau verstehen, welche Art von Risiko sie darstellen. Schwachstellenmanagement umfasst die Identifizierung, Priorisierung und Behebung von Sicherheitslücken. Getreu dem Motto »Was man nicht messen kann, kann man auch nicht meistern« haben mittlerweile viele Unternehmen erfolgreich ein systematisches Schwachstellenmanagement implementiert, das folgende sechs Schritte umfasst:

- Entdeckung: Identifizierung und Erkennung von Geräten, Systemen und Netzwerktopologien, um die ständigen Veränderungen in Netzwerken verfolgen zu können.
- Priorisierung von Assets: Bestimmung des geschäftlichen Werts der einzelnen Systeme und Anwendungen und Zuweisung entsprechender Prioritätsstufen. Die Netzwerk-Sicherheitsteams sollten dann die Prioritätenreihenfolge von Reparaturmaßnahmen danach festlegen, wie kritisch eine Ressource für das Unternehmen ist.
- Bewertung und Analyse: umfassende Analyse von Systemen und Entscheidung, wie kritisch und ernst zu nehmend Sicherheitslücken und die Anfälligkeit für Angriffe sind. Anhand dieser Informationen lässt sich leichter entscheiden, welche geschäftlichen Ressourcen in Gefahr sind und was vorrangig geschützt werden muss.
- Abhilfe: Beseitigung identifizierter Sicherheitslücken durch Rekonfiguration, Update oder Patchen der Systeme. Manchmal bieten Workarounds eine vorübergehende Lösung.
- Verifizierung: Validierung der Patches und Workarounds, um sich zu vergewissern, dass die Sicherheitslücken auch wirklich korrekt geschlossen wurden.
- Policy-Compliance: Beurteilung und Berichterstattung gemäß Security-Policies und Compliance-Anforderungen wie HIPAA und Sarbanes-Oxley sowie gemäß branchenspezifischen Vorgaben.

Basierend auf der jeweiligen Security-Policy eines Unternehmens, ist es ratsam, das Schwachstellenmanagement als umfassende, unternehmensweite Maßnahme zu implementieren. Dabei sollte der Grad der Bedrohung, die eine Sicherheitslücke für ein Unternehmen darstellt, die Art der Reaktion bestimmen. Als Leitlinie für den Prozess dienen folgende Fragen: Kann die Sicherheitslücke von jedem System im Netz aus ausgenützt werden, oder ist dazu ein Benutzerkonto auf dem Zielsystem erforderlich? Wurde bereits Exploit-Code in Umlauf gebracht? Welche geschäftlichen Ressourcen sind von der Sicherheitslücke betroffen? Diese Faktoren gestalten sich in jeder Situation anders und bestimmen den Bedrohungsgrad einer Sicherheitslücke innerhalb eines spezifischen Bereichs. Häufig werden Benchmarks wie die SANS/FBI Top 20 angewendet, um die spezifische Sicherheitsanfälligkeit eines Bereichs zu messen.

Exploits aus Geschäftssicht

Sicherheitslücken haben auf Unternehmen jeder Größe messbare Auswirkung. Wenn auf Grund eines Angriffs kritische Systeme nicht verfügbar sind und auf Daten nicht zugegriffen werden kann, entgehen einem Unternehmen wertvolle Geschäfte. Viele Firmen implementieren Schwachstellenmanagement als präventive Maßnahme, die eng mit einer übergreifenden Strategie des Risikomanagements verknüpft ist. Damit die Sicherheitsverantwortlichen die nötige Rückendeckung erhalten, muss die Unternehmensspitze in diesen Prozess eingebunden werden. Über die Sicherheitslage wird laufend auf der Führungsebene – in manchen Unternehmen sogar auf der Board-Ebene – informiert. Vor allem die Kenntnis der längerfristigen Entwicklung der Sicherheitsanfälligkeit ist ein äußerst wertvolles Instrument, um Investitionen in die Sicherheit zu rechtfertigen und zu belegen, dass diese sich ausgezahlt haben. Weitere Triebkräfte für die Implementierung eines konsequenten Schwachstellenmanagements sind gesetzliche und aufsichtsrechtliche Vorgaben. Insbesondere in Branchen, in denen die Vertraulichkeit und Integrität von Informationen absolut unerlässlich sind (beispielsweise im Finanz- oder Gesundheitswesen oder in ähnlich kritischen Bereichen), führen Unternehmen regelmäßig Schwachstellen-Audits durch, um die Einhaltung der rechtlichen Vorgaben zu überprüfen und die notwendige Berichterstattung vorzunehmen. Darüber hinaus führt der Trend hin zum Outsourcen von IT-Systemen und -Abläufen zu einer verstärkten Implementierung von Security-Service-Level-Agreements (SLAs), bei denen der Outsourcing-Provider hinsichtlich des Patchens von Sicherheitslücken genau definierte Metriken einhalten muss. Schwachstellenmanagement-Verfahren und Sicherheitsaudits sind unabdingbare Maßnahmen, um die Einhaltung solcher SLAs zu überprüfen und durchzusetzen. Eine hundertprozentige Sicherheit wird das Unternehmen bei all diesen Anstrengungen aber nicht erreichen.

Dr. Gerhard Eschelbeck,
CTO und VP-Engineering bei Qualys